DEPARTMENT OF THE NAVY
NAVAL SUPPLY SYSTEMS COMMAND
5450 CARLISLE PIKE
PO BOX 2050
MECHANICSBURG PA 17055-0791

TELEPHONE NUMBER
COMMERCIAL
AUTOVON
IN REPLY REFER TO:

5000
Ser 00e/017
January 10, 2002

MEMORANDUM FOR NAVY CHIEF INFORMATION OFFICER

Subj: DRAFT DON CAC POLICY STATEMENT

Ref: (a) DON CIO E-Mail of 14 Dec 01 (w/attachment)

Encl: (1) Revised Draft DON CAC Policy Statement

1. Reference (a) forwarded the initial DON CAC Policy Document for review by DON eBusiness Operations Office (eBUSOPSOFF) Smart Card and Common Access Team at the direction of Barbara Hoffman.

2. Considerable time and effort have been invested in reviewing and proposing constructive changes to this document. These changes are confined specifically to DON coverage of Smart Card Technology and associated interface issues. Management, control, and proliferation of technology and policy supporting standalone eBusiness initiatives and applications are not considered part of this scope. It is our intent to provide additional definition, clarity, and separation among the major organizational entities presented in the source draft. Revisions, to include organizational roles outlined in the DON eBUSOPSOFF Charter and transition MOA have been incorporated.

3. A relationship diagram depicting the many organizational linkages proposed in this Policy Statement draft can be found at the end of the Roles and Responsibilities section.

4. The following significant issues have been changed from the initial draft:

(1) That DON eBUSOPSOFF assume the role of "Technical Lead" for all DON Smart Card Technology matters.

(2) The concept of the DON Board of Representatives (BOR) chaired by a DON CIO Flag/SES to review each submission for space apportionment of the CAC using risk factors such as mission need, cost, schedule, and performance may not be necessary. These review and analysis functions can be staffed by the eBUSOPSOFF and submitted to DON CIO.

(3) The concept of establishing an eBusiness Working Group as a representative individual command voice comprised of stakeholders across DON claimants can be accommodated by the existing DON AIT Steering Group. The intent is to ensure that the eBUSOPSOFF is providing value added services to users.

(4) Afloat access control - eBUSOPSOFF is in the process of transferring afloat Quarterdeck Access Systems to SPAWAR, PMW-151, as the program manager of NTCSS programs of record. We recommend omitting references to specific applications in the document.

(5) A shift in responsibility from NPC-3/HQMC to DON eBUSOPSOFF.

5. It is recognized that the changes proposed are expansive, however necessary to establish necessary guidance that responds to potential users of this technology and lays down an unbroken line of responsibility and expectation for all participating parties. A summary of changes to this draft proposal would be appreciated by 15 February.

Very Respectively,

KAREN E. MELOY
Assistant Deputy Commander
DON eBusiness Operations Office

Department of the Navy Smart Card Technology Policy Statement

Purpose

This document establishes policy for the implementation of Smart card Technology (SCT) in the Department of the Navy (DON). Associated roles and responsibilities of Department of Defense (DoD) and DON organizational entities are delineated as appropriate.

Introduction

In a memorandum dated 10 November 1999, the Deputy Secretary of Defense (DEPSECDEF) directed that smart card technology be utilized within the Department, and that the Common Access Card (CAC) become the common platform for implementation of this technology. The memo directed that the CAC be used as the hardware token for Public Key Infrastructure (PKI) credentials and that it be issued to all DoD personnel. The Department of the Navy has embarked on an aggressive enterprise-wide plan to implement SCT throughout the Navy and Marine Corps. It is intended that this technology be fielded with the capacity to support seamless ship-to-shore web-based information technology (IT) network architectures, within a standardized physical and logical security infrastructure, and that the CAC be used as a key component in the migration to automated eBusiness-based solutions.

The DEPSECDEF memo directed that the multi-technology Common Access Card (CAC) become the new DoD Identification Card. The CAC replaces DD Form 2 Teslin ID cards, and will be issued through the Defense Enrollment Eligibility Reporting System/Real-Time Automated Personnel Identification System (DEERS/RAPIDS) to the following personnel:

- Active Duty Uniformed Services
- Selected Reserve
- DoD Civilian Employees
- Eligible DoD Contractors

The CAC will be the primary enabler for physical identification of the holder, secure authentication and access to IT networks, and physical security systems. Technologies currently residing on the CAC include:

- Integrated Circuit Chip (ICC) with embedded crypto-coprocessor
- Magnetic stripe with three standard tracks
- Barcode schemes to store permanent information
- Photograph and basic identification information

It is essential that DoD have the ability to protect the value and integrity of its information, and control access to authorized users. As a hardware token, the internal architecture of the CAC has been designed to securely store PKI certificates within the crypto-coprocessor. Used in conjunction with a Personal Identification Number (PIN) for log-on, the PKI will also enable email authentication, digital signing, encrypting/

decrypting and access to secure web sites. Compatible web-based IT architectures, to include the Navy/Marine Corps Intranet (NMCI) ashore, Integrated Shipboard Network Systems (ISNS), Task Force WEB, Marine Corps Enterprise Network (MCEN), and the Marine Corps Tactical Data Network (MCTN), will utilize the CAC as the secure key. New capabilities and functionality will be incorporated as technology and requirements evolve.

Background

In 1996, DON began to actively implement SCT in Navy and Marine Corps operational and training environments. Since June 1998, recruits have used SCT in daily activities at both Navy and Marine Corps Recruit Training Commands/Depots. Navy and Marine Corps personnel on the island of Oahu rely on smart cards as a normal business practice for food service, weapons issuance, and manifesting for major exercises across the Pacific Rim. Both the Navy and Marine Corps have realized cost reductions, improvements in operational efficiency, enhanced mission readiness, and improved quality of life using multiple technology smart card systems during an extended demonstration period. Utilization of the smart card applications has not migrated outside pilot and prototype sites ashore; enterprise-wide acceptance of SCT awaits smart card issuance to all eligible users.

During the spring of 1999, SCT was introduced to the USS GEORGE WASHINGTON and USS KITTY HAWK Carrier Battle Groups (CVBG), their associated Carrier Air Wings (CVW), the USS SAIPAN and USS BELLEAU WOOD Amphibious Ready Groups (ARG), and their Marine Expeditionary Units (MEU). The DON has leveraged lessons learned from these initiatives, and others, to move away from storing large amounts of data on the card, toward a web-enabled information system that can be globally accessed by authorized CAC recipients.

Development of backwards compatibility capability for existing Smart card applications, as they transition from the current smart card environment to the CAC, will be managed by the DON eBusiness Operations Office (eBUSOPSOFF), an organization chartered under Naval Supply Systems Command, and located in Mechanicsburg, PA. The organizational and operational charter for the DON eBUSOPSOFF was approved and signed by SECNAV 21 September 2000; the organization began operations 01 October 2001. The DON eBUSOPSOFF receives policy guidance from DON CIO and is tasked with identification and implementation of business strategies, technologies, process automation, and system integration. System improvements, including pilot/prototype fielding of new, fully integrated technologies and business systems will be encouraged as DON Functional managers study existing manual, paper intensive, and stove piped process and systems. As issuance of CACs to Navy and Marine Corps personnel on Oahu begins, applications for food service, manifest tracking, warrior readiness, and weapons issuance will be made backward compatible to the CAC.

In its capacity as the Functional Manager and technical lead for implementation of Smart card technology for DON, eBUSOPSOFF is chartered to lead and manage the issuance of the CAC throughout the Department – initial CAC issuance and subsequent versions as technical upgrade and refreshment occur. In this capacity, the eBUSOPSOFF staff must work with all levels of the chain of command in both the Navy and Marine Corps. Additionally, the eBUSOPSOFF must work with all other Functional Managers as CAC/SCT technology is integrated into legacy level applications and software systems, and with major information technology systems of record throughout the Department.

Roles and Responsibilities
(Relationships among responsible entities are provided in a diagram following this section.)

DoD Electronic Business Board of Directors (eB BoD) serves as the single DoD senior board for eBusiness and is subordinate to the DoD CIO Executive Board. The Board is responsible, but not limited to setting Department priorities, cross functional/cross Component solution approaches, and performance measures. The eB BoD will assure the integration of functional requirements and determine summary level chip storage allocations, to include those for Component specific use of the CAC. The eB BoD will be chaired by the DoD Deputy CIO and include representatives (Flag/SES minimum) from affected Principal Staff Assistants (PSAs) within the Office of the Secretary of Defense (OSD) and the DoD Components, and will oversee the operation of the Smart card Senior Coordinating Group (SCSCG). The Board will meet at least quarterly.

Smart Card Senior Coordinating Group (SCSCG) shall:
Implement DoD interoperability standards for SCT and plan to optimize use of SCT as a means to enhance readiness and improve business processes. The SCSCG will accomplish this responsibility by coordinating the resolution of DoD Component requirements with the DoD PKI Program Management Office (PMO), and making recommendations to include the impact of Joint Technical Architecture to the DoD CIO through the eB BoD. The SCSCG will make recommendations for technology upgrades and technologies to be included in future generations of the CAC. The SCSCG provides technical direction to the Defense Manpower Data Center, Access Card Office (DMDC ACO) concerning implementation of the CAC and subsequent upgrades, changes, technology refreshment, and implementation timelines. The SCSCG Charter provides, that the Secretary of the Navy shall appoint the Flag/SES SCSCG Chair and lists Group composition. Meetings will be held at least four times a year at the discretion of the Chair.

Defense Manpower Data Center, Access Card Office/DEERS RAPIDS Organizational Division (DROD) shall:
Plan, program, acquire, field, and integrate the DOD CAC. The ACO will provide DoD Components operational, technical, program, and policy support associated with CAC issuance, eligibility, functionality, and future development. Specific responsibilities and functions are outlined in the DoD Configuration Management Plan. The ACO Director will serve as executive secretary to the eB BoD and SCSCG.

augmented by industry experts. The eBUSOPSOFF will serve as the DON champion for change and implementation focal point for DON CAC/SCT initiatives. The following program areas will be the responsibility of the eBUSOPSOFF:

(1) Program Support

(a) Serve as advocate for field activities and installations affected by implementation of CAC/SCT to DON and DoD policy-making organizations.

(b) Manage and coordinate DON interface development, working with DON functional managers to satisfy requirements within program, policy, and approved technology constraints. Assure all formal program documentation is completed, submitted and approved.

(c) Coordinate and staff DON data requirements for interface development with the SCSCG for approval.

(d) Coordinate and staff for approval other Service and Agency requests for application interface data requirement development as directed by the SCSCG. Submit coordinated DON response to these requests to other Services, Agencies, and SCSCG.

(e) Develop and maintain all DON technical documentation associated with DON implementation of CAC/SCT technology. Manage DON implementation of all policy, programmatic and procedural directives associated with CAC/SCT.

(f) Manage CAC/SCT fielding; provide advisory services to the Department on implementation of CAC/SCT technologies and initiatives.

(g) Maintain DON demographics information necessary to manage the placement of DEERS/RAPIDS workstation infrastructure for the Department in support of CAC issuance, and technology refreshment, changes and upgrades. Coordinate DON implementation of DoD policies pertaining to DEERS/RAPIDS workstation and infrastructure utilization and business rules associated with workstation placement

(h) Provide consulting services for DON organizations implementing CAC/SCT solutions to include information assurance considerations, DON architecture, and interoperability standards.

(i) Support functional policy managers in developing CAC/SCT Implementation Plans in support of the DON CAC/SCT Strategic Plan.

(j) Provide Public Affairs guidance and material to DON sites receiving the CAC. Create and maintain a web site with CAC information. Serve as a responsive focal point where CAC users can direct questions and concerns to the DON eB Operations Office.

(k) Formulate agreements with the DON Automated Identification Technology (AIT) Steering Group and PKI Users Group to monitor the value of services provided to users.

(2) Issuance

(a) Serve as the DON principal liaison with the DMDC ACO in matters pertaining to CAC issuance, DEERS/RAPIDS workstation placement, installation and upgrade, DEERS/RAPIDS software change management and implementation throughout DON, and implementation of future-generation CAC technology.

(b) Manage DON card stock and program consumables in coordination with DMDC.

- Technical and Program Evaluation (budget requirements, Program Objective Memorandum submission)
- Development of requirements
- Application development and testing (this may also include card hosted applications and interfaces)
- Integration (with new or existing systems)
- Fielding (includes training and rollout scheme)
- Configuration management

Assistant Secretaries of the Navy (FM&C, RDA, I&E, M&RA), CNO and CMC shall:

(1) Work with the DON CIO to instill CAC/SCT concepts and technologies throughout DON.

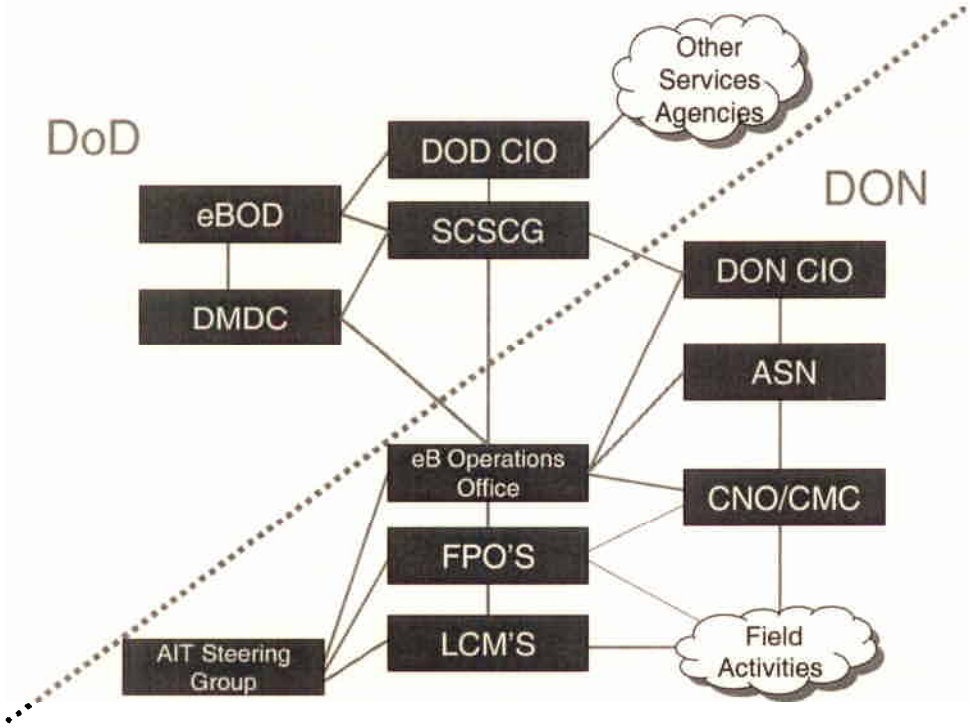
(2) Apply CAC/SCT best practices to the maximum extent practical to improve both combat support capabilities and DON business operations.

(3) Ensure the insertion of CAC/SCT capabilities into the development, modernization, expansion or prototype of systems that interface with DON business partners and Functional Process Owners.

(4) Support the development and updating of the DON CAC/SCT Strategic and Implementation Plans.

(5) Support CAC/SCT standardization efforts.

(6) Direct CAC/SCT implementation at respective subordinate Commands.



Relationship Diagram

implementation occurs concurrent with systems upgrades occurring under the ISNS Program. Classified networks are not addressed within this policy.

Summary Guidance

The CAC will ultimately replace traditional unclassified DoD ID cards associated with physical and logical access. The CAC is the first enterprise-wide fielding of Smart card technology. The CAC will replace traditional military, Civil Service, and authorized contractor ID cards and designated physical security access passes. However, the initial version of CAC does not accommodate all of the requirements of the DON. As supporting technologies evolve, the CAC will support additional requirements and functional applications as directed by the SCSCG or recommended by other DoD Component-specific Configuration Management Boards.

Future generations of the CAC are envisioned to provide contactless technology for use in physical access control systems, and in other systems where passive interrogation of an ICC is preferable to current contact processes.

This policy guidance will be reviewed and revised on an annual basis.

Waivers

DON CIO will only consider written request for waivers to this policy. Requests must be submitted through Command channels to the eB Operations Office for endorsement and forwarding to DON CIO.

QAS	Quarterdeck Access System
RAPIDS	Real-Time Automated Personnel Identification System
RDA	Research, Development, and Acquisition
SCSCG	Smart Card Senior Coordinating Group
SCT	Smart Card Technology
SES	Senior Executive Service
SPAWAR	Space & Naval Warfare Systems Command
SYSCOM	System Command